



**UNCLASSIFIED**



# **North Dakota Homeland Security Anti-Terrorism Summary**



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners. If you have any comments to improve this summary or local information you would like to see in the summary please send the information to; [kihagel@nd.gov](mailto:kihagel@nd.gov)

**UNCLASSIFIED**

## **QUICK LINKS**

**North Dakota**

**Regional**

**National**

**International**

**Banking and Finance Industry**

**Chemical and Hazardous  
Materials Sector**

**Commercial Facilities**

**Communications Sector**

**Critical Manufacturing**

**Defense Industrial Base Sector**

**Emergency Services**

**Energy**

**Food and Agriculture**

**Government Sector (including  
Schools and Universities)**

**Information Technology and  
Telecommunications**

**National Monuments and Icons**

**Postal and Shipping**

**Public Health**

**Transportation**

**Water and Dams**

**North Dakota Homeland Security  
Contacts**

## **NORTH DAKOTA**

**FEMA moves out emergency supplies.** With the 2010 Red River flood fight winding down, the Federal Emergency Management Agency trucked emergency supplies for 20,000 potential flood victims out of North Dakota. The trucks, which have been at Grand Forks Air Force Base since March 19, were moved to national logistical caches for possible use in other areas, including the flood disaster unfolding in the Northeast. The supplies include emergency generators, communications equipment and enough cots, blankets, personal hygiene kits and food to accommodate 20,000 refugees for five days. Meanwhile, FEMA is launching another phase of its flood-recovery program in North Dakota. On Monday, disaster teams will begin working with county, city and township officials to obtain federal funding to repair or replace damaged public infrastructure during the flood disaster. Source:

<http://www.grandforksherald.com/event/article/id/156471/>

# UNCLASSIFIED

**Fargo levees coming down starting Friday.** Clay levees that protected City of Fargo property during this spring's flood threat will start to come down Friday. Workers will start with the dike along Second Street North just to the east of City Hall. After that, it is the dikes along Second Street South by the Fargo High Rise and Oak Street North. City officials hope to have the First Avenue North bridge reopened by Monday. Source: [http://www.kfgo.com/news\\_Detail.php?ID=10729](http://www.kfgo.com/news_Detail.php?ID=10729)

## **REGIONAL**

**(Minnesota) Minnesota firm recalls ham products for possible Listeria contamination.** Lorentz Meats, a Cannon Falls, Minnesota establishment, is recalling approximately 100 pounds of ham products that may be contaminated with *Listeria monocytogenes*, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced April 4. Various sizes of whole or half ham packages of "KOWALSKI'S Markets, FULLY COOKED, SMOKED HAM, Naturally Smoked with Hardwoods, KEEP REFRIGERATED." Each package bears a freeze by date "FREEZE BY 05/14/10" as well as the establishment number "Est. 21207" inside the USDA mark of inspection. The ham products were produced on March 12, 2010, and were distributed to retail establishments in Minneapolis/St. Paul, Minnesota, and the surrounding area. The problem was discovered through third-party testing, and the establishment notified FSIS. FSIS has received no reports of illnesses associated with consumption of this product. Source:

[http://www.fsis.usda.gov/News\\_&\\_Events/Recall\\_022\\_2010\\_Release/index.asp](http://www.fsis.usda.gov/News_&_Events/Recall_022_2010_Release/index.asp)

**(Minnesota) Vandals cause sewage overflow in Duluth.** Logs, boulders and other debris were thrown into the sewer line, resulting in an obstruction and subsequent estimated overflow of about 21,500 gallons into Miller Creek. An LSC student discovered the overflow Wednesday afternoon and reported it to authorities. "It appears that the vandals pried off at least one manhole cover in the wooded area along Miller Creek and threw in whatever they could find in the vicinity," said The Western Lake Superior Sanitary District's (WLSSD) manager of Planning and Technical Services. "Our crews found a substantial amount of logs, boulders and other debris in the line. To prevent this from happening in the future, all manhole covers in this area will be replaced with a type that makes their removal more difficult and will deter future tampering. Additionally, we'll be taking other measures to secure the covers in place." WLSSD experienced a similar event in 2007 and replaced about 20 covers in the area at that time. WLSSD staff and contractors cleared the obstruction and restored flow by 9:45 last night. WLSSD staff is cleaning up the overflow area and no long-term environmental effects are anticipated. "Removing manhole covers creates environmental and public health hazards and also creates unsafe conditions. Manhole covers are heavy and can pose a danger if dropped. Open manholes also create fall hazards. We are fortunate that no one got hurt," said the manager. Clearing this obstruction will cost us more than \$5,000." If the parties responsible for this vandalism are identified, WLSSD will pursue all appropriate legal remedies to the fullest extent of the law.

Source: <http://www.northlandsnewscenter.com/news/local/89695692.html>

**(Minnesota) Hwy. 10 bridge north of Little Falls to be replaced.** The Minnesota Department of Transportation (MnDOT) plans to rebuild the Highway 10 bridge over the Mississippi River in Little Falls this construction season after an ice jam damaged the bridge a couple weeks ago. Mn/DOT closed the bridge March 17, 2010 after an ice jam caused extensive damage and flood waters overflowed the bridge. The bridge has since been reopened, but bridge repairs would cost around \$1.5 million. Rebuilding the bridge completely will cost about the same as repairs. Crews are already

# UNCLASSIFIED

## UNCLASSIFIED

working on the bridge and plan to finish the entire project by the end of this construction season. The new bridge will have a bigger opening underneath to prevent ice jam and flooding damages from happening in the future. Two of the four lanes on the bridge are still open to traffic. Those lanes will remain open during the entire construction season. The completion date for rebuilding the bridge has not been set. The new bridge will last about 60 years. Source:

<http://ksax.com/article/stories/S1494094.shtml?cat=10230>

### **(South Dakota) Scam artists using census to try and get bank account, Social Security numbers.**

South Dakotans are being cautioned about a scam circulating under the guise of a 2010 census form. The state attorney general's office says official-looking requests for financial information are not part of the census. Scam artists have sending letters and e-mails and even showing up at homes seeking Social Security numbers and information about bank accounts. The attorney general's office says the census does not ask for that information, and residents should not give it out. Source:

<http://www.argusleader.com/article/20100401/UPDATES/100401035/-1/DATABASE0202>

**(Minnesota) Credit card skimmer used at US Bank ATM in Eden Prairie.** Police in Eden Prairie, Minnesota, are warning of credit card skimmers at ATM machines after a card scanner fell off a machine earlier this month. According to Eden Prairie police, a consumer was using an ATM at the US Bank at 300 Prairie Center Drive on March 19 when the scanner fell off. Police said the scanner was actually a skimming device attached by someone attempted to steal card information. Customers using an ATM cannot notice a difference because the card simply passes through the skimmer and then enters the actual bank scanner in the ATM. Victims still receive their money, with no sign their financial information has been compromised. Police say credit card skimmers are also in play through criminal groups getting servers hired at local restaurants to steal card information. Two similar cases have popped up in the Twin Cities metro this year — one involving a St. Louis Park Olive Garden server , and the other involving a Coon Rapids TGI Friday's server. The suspects in those cases stole thousands of dollars from unsuspecting victims using skimmers. Source:

<http://www.myfoxtwincities.com/dpp/news/minnesota/eden-prairie-atm-credit-card-skimmer-mar-30-2010>

**(Minnesota) MN money manager charged in \$190M Ponzi scheme.** An Apple Valley money manager is charged with orchestrating a Ponzi scheme that allegedly defrauded at least 1,000 victims out of \$190 million. The 37-year-old suspect was charged on March 30 in federal court in Minneapolis with mail fraud and tax evasion. The charges say that from July 2007 to July 2009, the suspect told clients he had invest their money in a foreign currency trading program with annual returns of 10 to 12 percent. Instead, officials say, he used the money for personal expenses and to keep the scheme going. The suspect's attorney told The Associated Press Wednesday that a plea agreement has been reached with prosecutors. Source: <http://www.wqow.com/Global/story.asp?S=12233886>

## **NATIONAL**

**Mexico, parts of U.S. hit by major quake.** A 7.2 magnitude earthquake rocked Mexico and parts of the Western United States on Sunday, leaving at least two dead and 100 injured according to early media reports. It was reportedly the most powerful quake to strike the region in decades. According to the U.S. Geological Survey, the earthquake occurred at 3:40pm and was centered just outside of Mexicali, where both fatalities occurred. The 40-second earthquake "shook tens of millions of people

## UNCLASSIFIED

# UNCLASSIFIED

across two countries and three states swaying high-rise buildings from Los Angeles to Las Vegas and the border town of Tijuana,” according to UK’s Mail Online website. “In California, Disneyland rides were closed and inspected for damage and several historic hotels were evacuated as a precautionary measure.” Three aftershocks followed within the hour following the initial earthquake. Those aftershocks had magnitudes of 5.1, 4.5, and 4.3, and were followed by smaller tremors later on in the day. A member of the U.S. Geological Survey warned that more seismic activity may follow. Source:

[http://www.redorbit.com/news/science/1845367/mexico\\_parts\\_of\\_us\\_hit\\_by\\_major\\_quake/](http://www.redorbit.com/news/science/1845367/mexico_parts_of_us_hit_by_major_quake/)

## **INTERNATIONAL**

**Blasts target Baghdad embassies.** Suicide attackers have detonated three car bombs near embassies in Baghdad, killing at least 42 people and wounding more than 200 in back-to-back attacks.

Authorities say they foiled two other attacks aimed at diplomatic targets. A spokesman for the city’s operations command center said the blasts went off within minutes of each other — one near the Iranian Embassy and two others in an area that houses several embassies, including the Egyptian Consulate, German, and Spanish embassies. The rise in bloodshed after a relative lull deepened fears that insurgents are seizing on the political uncertainty after last month’s close parliamentary elections to sow further instability. TV footage showed civilians outside the Iranian Embassy loading casualties into police vehicles and ambulances. Source:

[http://www.google.com/hostednews/ukpress/article/ALeqM5g2ce0UWgIbztP-6vBOwpzP9\\_CTgQ](http://www.google.com/hostednews/ukpress/article/ALeqM5g2ce0UWgIbztP-6vBOwpzP9_CTgQ)

**South Korea warship pursuing oil tanker hijacked by pirates off Somali coast.** South Korea sent a warship to the Indian Ocean on Monday to pursue Somali pirates who hijacked a U.S.-bound oil tanker in another brazen assault in shipping lanes hundreds of miles off the Horn of Africa. Korean officials said the hijacked ship, the Samho Dream, is a 300,000-ton tanker, but they gave no indication how much oil was on board when pirates seized the vessel Sunday about 950 miles off the Somali coast. The crew of five Koreans and 19 Filipinos was sailing from Iraq to Louisiana. “The government has dispatched our Cheong-hae naval unit to the waters of the Indian Ocean, where the ship hijacked by Somali pirates is assumed to be,” the Foreign Ministry said in a statement, referring to a destroyer that is part of the nation’s anti-piracy fleet. Source:

<http://www.latimes.com/news/nationworld/world/la-fg-korea-somali-pirates6-2010apr06,0,5809806.story>

**Gunmen kidnap Total oil worker in Nigerian delta.** Gunmen kidnapped an employee of the French oil company Total in Nigeria’s Niger Delta on March 31, police said. The Nigerian worker was abducted after leaving his home in Port Harcourt, the main city in the OPEC member’s restive oil-producing Niger Delta. “A Nigerian employee of Total was abducted by unidentified gunmen this morning on his way to work and driven in a getaway car, said a spokeswoman for Rivers state police. Kidnappings for ransom, armed robbery and carjackings are common in the Niger Delta, where poverty is widespread despite its vast oil and gas reserves. Most victims are released unharmed after payment of a ransom.

Source: <http://news.alibaba.com/article/detail/markets/100270886-1-gunmen-kidnap-total-oil-worker.html>

# UNCLASSIFIED

## **BANKING AND FINANCE INDUSTRY**

**Guide released to mitigate damage of cyberattacks.** Two industry groups on March 31 released a free guide that the authors hope will encourage financial executives within an organization to take the lead role in mitigating cyber-risks. The framework, developed by the Internet Security Alliance (ISA) and the American National Standards Institute (ANSI), comes in response to the White House's release in May 2009 of the 60-day Cyberspace Policy Review. That report stated that between 2008 and 2009, American business losses due to cyberattacks grew to more than \$1 trillion in intellectual property. The new publication, The Financial Management of Cyber Risk: An Implementation Framework for CFOs, helps organizations meet one of the review's recommendations that monetary value be assigned to cyber-risks and their consequences. One of the main challenges is to make senior executives aware of the impact data theft and other consequences of cyberattacks can have on a company's bottom line, the president of the ISA told SCMagazineUS.com on April 1. Source: <http://www.scmagazineus.com/guide-released-to-mitigate-damage-of-cyberattacks/article/167149/>

**(Florida) 2nd suspicious package at bank.** The Palm Beach County Sheriff's Office returned to a Chase bank at 328 Northlake Boulevard after a second suspicious package was found in the afternoon of April 1. In the morning of April 1, the bank was evacuated as a precaution. The Palm Beach County Bomb Squad and fire rescue set up a staging area in a nearby Publix shopping center. The investigation started when a box with wires sticking out of it was found at the bank. The package was later destroyed and those evacuated were allowed to return. A second suspicious package turned up in the after afternoon around 4 p.m. West Palm Beach Police had received a bomb threat at a Chase bank on March 31 but no location was given. Source: <http://www.wptv.com/content/news/centralpbc/story/Suspicious-package-found-at-bank/HDYC8Jl-JUKmBNt3y4VOeA.cspX>

**(Ohio) FBI: Million-dollar credit card fraud ring busted in Cleveland.** The FBI announced the arrest of eight men, charged with using other people's credit card information to buy as much as a million dollars in merchandise from Northeast Ohio stores. "These are stores that we all frequently visit with store credit cards that many of us carry in our wallets," said the special agent in charge of the Cleveland division of the FBI. He named Lowe's, Home Depot, Staples, Best Buy, hhgregg, Macy's, Nordstrom, Saks Fifth Avenue, and Sears as among the local stores victimized. In the scheme, the FBI says an inmate at a federal prison in Fort Dix, New Jersey, used a cell phone to access and alter existing credit card accounts. They say he fraudulently added new users to other people's accounts, and that the new users would make big-ticket purchases at Northeast Ohio stores. The FBI says the prisoner was persistent in calling customer service departments until he was successful in gaining access to someone else's personal or business account. He would then modify the account and make one of the Cleveland men authorized users. At times he would use bits and pieces of public information, and use either guesswork or persistence, to finally gain access to the credit card accounts, according to the FBI. Source: [http://www.wkyc.com/news/local/news\\_article.aspx?storyid=133530&catid=3](http://www.wkyc.com/news/local/news_article.aspx?storyid=133530&catid=3)

## **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

Nothing Significant to Report



## **COMMERCIAL FACILITIES**

**(New York) 4 shot, 54 arrested in Times Square Easter melee.** Four people were shot and 54 were arrested in New York's Times Square late Sunday night in an Easter melee some fear was gang-related. Shots rang out as groups of young people charged through the streets of Manhattan, frightening bystanders and prompting some businesses to close early to avoid being ransacked. It is unclear whether the victims were innocent bystanders or part of the groups of young people flooding the streets. The mayhem covered nearly a mile, from Herald Square to Rockefeller Center to the bright lights of tourist-filled Times Square. Hundreds of New York City police officers worked to contain the violence, making dozens of arrests and stopping pedestrians to look for weapons, the New York Post reported. One police officer was injured in the knee as he tried to stop the ruckus. A couple of hours later, two more women were shot and suffered non-life-threatening injuries, The Associated Press reported. Even before the young people hit the streets, the cops were waiting for them in Times Square. Apparently, the violence is a kind of Easter Sunday tradition for New York gangs. According to some police officers, business owners, and New York urban legend, the holiday is also known as "Gang Initiation Day" among the city's gang-bangers. Source:

<http://www.aolnews.com/crime/article/4-shot-54-arrested-in-times-square-easter-melee/19426450>

**(Pennsylvania) Police believe teens responsible for series of explosions in Newtown.** Police believe a group of teens are responsible for three explosions which occurred at two Newtown Borough businesses and at a Newtown Township fast-food restaurant Tuesday afternoon. The first was reported at 3:15 p.m. at the CVS Pharmacy at on South Lincoln Avenue where police said a device was detonated inside the store. Police said a customer was taken by ambulance to St. Mary Medical Center and one employee transported himself to the medical center where he was treated for nose and throat irritation. Employees evacuated all customers from the store. Inside, Newtown Borough police found remnants of what they described as an "improvised explosive device" in one of the aisles and obtained images and video from the store's security system. Police said a person of interest was observed on the video. At about the same time as the CVS incident, police said something exploded in a trash can located inside the front door of a Starbucks Coffee at on South State Street. There were several patrons inside the store at the time of the explosion. The assistant manager told police that several young men had entered the store before the explosion. They did not purchase anything and left just after the explosion, exiting out of the back door, police said. The manager told police she could identify the three males. Police in neighboring Newtown Township reported a similar incident, also on Tuesday, at the Wendy's Restaurant off of Swamp Road. According to police, a bottle bomb went off at the rear of the building. Police are investigating the incidents and are expected to file charges. Source:

[http://www.buckslocalnews.com/articles/2010/04/01/the\\_advance/news/doc4bb39b70a4ac3227677407.txt](http://www.buckslocalnews.com/articles/2010/04/01/the_advance/news/doc4bb39b70a4ac3227677407.txt)

## **COMMUNICATIONS SECTOR**

**US, Europe, Japan agree on data center efficiency metric.** Industry groups and government agencies from the U.S., Europe and Japan have reached a basic agreement on how to measure the energy efficiency of data centers, they are expected to say on April 5. The agreement is seen as significant because it establishes a common metric that different types of data centers, in different parts of the

# UNCLASSIFIED

world, can use to report their level of energy efficiency. That could provide a yardstick for companies to assess the efficiency of their own data centers, and also to gauge the effectiveness of energy-saving techniques employed by other facilities. The agreement is unusual for its level of international cooperation. Orchestrated by the Green Grid, an industry consortium in the U.S., the agreement is backed by the U.S. Department of Energy, the U.S. Environmental Protection Agency, the European Union Code of Conduct and the Japan Ministry of Economy, according to a statement from the Green Grid. Source:

[http://www.computerworld.com/s/article/9174701/US\\_Europe\\_Japan\\_agree\\_on\\_data\\_center\\_efficiency\\_metric](http://www.computerworld.com/s/article/9174701/US_Europe_Japan_agree_on_data_center_efficiency_metric)

**Earthquakes and data centers.** The April 4 magnitude 7.2 earthquake in Baja California was felt in large portions of Southern California. It rattled nerves and shook up some equipment as well. "Our data center had servers rolling back and forth on earthquake gliders," reported the manager at ProtectRite of Encinitas, California (a San Diego suburb) on his Twitter stream. "It was intense â\_! All employees working today ran to parking lot. Pictures toppled on desks and server safety systems engaged." Earthquake gliders? Many data centers use seismic isolation technology to protect racks and servers in the event of a major earthquake. Last year a representative of WorkSafe provided a demonstration of his company's ISO-Base platforms, which sit under the data center racks and allow them to shift independently of the building during an earthquake, reducing damage. WorkSafe has provided seismic isolation systems at data centers operated by Boeing and local governments in the Pacific Northwest, as well as many facilities in Japan. Source:

<http://www.datacenterknowledge.com/archives/2010/04/05/earthquakes-and-data-centers/>

## **DEFENSE INDUSTRIAL BASE SECTOR**

**Raytheon Joint Standoff Weapon C-1 conducts first captive-flight test.** Raytheon Company's Joint Standoff Weapon C-1 achieved a major milestone when it completed its first captive-flight test on an F/A-18E/F fighter aircraft. JSOW is a family of low-cost, air-to-ground weapons that employs an integrated GPS- inertial navigation system and terminal imaging infrared seeker that guide the weapon to the target. JSOW C-1 adds moving maritime target capability and the two-way Rockwell Collins Strike Common Weapon Datalink to the combat-proven weapon. Source:

[http://nosint.blogspot.com/2010/04/raytheon-joint-standoff-weapon-c-1.html?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed:+blogspot/fqzx+\(Naval+Open+Source+INTelligence\)](http://nosint.blogspot.com/2010/04/raytheon-joint-standoff-weapon-c-1.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/fqzx+(Naval+Open+Source+INTelligence))

**Congressmen worried about federal lab oversight.** Two Republican members of the House Energy and Commerce Committee are concerned the Department of Energy could be easing safety and security oversight at national laboratories. U.S. Representatives from Texas sent letters Monday to the Government Accountability Office and the Energy Secretary. They asked the GAO to review the proposed plan, which they say would allow contractors to implement safety and security programs without strong federal oversight. They say the Energy Department has suspended some independent inspections of nuclear weapons complex facilities and that dozens of internal reviews and assessments have been suspended in the past year. They say incidents at Los Alamos and Lawrence Livermore labs showed the need for safety and security improvements in the past decade. Source:

<http://www.newswest9.com/Global/story.asp?S=12232070>

# UNCLASSIFIED



# UNCLASSIFIED

**Lockheed Martin successfully tests Joint Air-To-Ground Missile (JAGM) tri-mode seeker.** Lockheed Martin has successfully completed a wide-ranging series of tests on the multi-mode seeker for its Joint Air-to-Ground Missile (JAGM) system. JAGM will provide a precision, adverse weather, low-collateral-damage weapon to rotary- and fixed-wing pilots, as well as the unmanned aerial system community. Currently in the technology development phase, JAGM's tri-mode seeker includes imaging infrared, semi-active laser and millimeter wave radar sensors for precision-strike targeting. Source: [http://nosint.blogspot.com/2010/04/lockheed-martin-successfully-tests.html?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed:+blogspot/fqzx+\(Naval+Open+Source+INTelligence\)](http://nosint.blogspot.com/2010/04/lockheed-martin-successfully-tests.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/fqzx+(Naval+Open+Source+INTelligence))

**GAO flags LCS missile problems.** One of the primary missions of the Littoral Combat Ship (LCS) is to act as a screen for larger fleet ships, fending off small boat swarms in coastal waterways. The standard package for that mission is the Surface Warfare module (SUW), which includes a 30mm cannon and the NLOS-LS, a missile system. According to a report released today by the auditors at the Government Accountability Office, the Navy took delivery of a SUW package in 2008, minus the launcher and missiles. GAO says the launcher was tested last summer, but failed due to a malfunctioning sensor and battery connector. The Navy expects delivery of another SUW package this year, this time with the launcher, but minus the missiles. Army officials said they think the missile's targeting problems are serious ones, considering how far along the NLOS-LS is in development. They've hinted they may look at a low cost alternative to the NLOS-LS. Yet the Navy is going ahead with delivery of the launcher. Absent a functioning SUW package, the LCS is not mission capable for its primary function as a small surface combatant. Source: <http://defensetech.org/2010/03/30/gao-flags-lcs-missile-problems/>

## **CRITICAL MANUFACTURING**

**GM to use brake safety measure worldwide.** General Motors says it will install a new brake safety measure that can prevent unintended acceleration on all its new vehicles worldwide by 2012. The step comes as federal regulators consider making the system mandatory on cars and trucks after Toyota's big problems with vehicles that can speed out of control. A brake override reduces power to the engine when the driver steps on both the brake and accelerator. It should also slow a vehicle if the gas pedal is stuck. GM has not had major problems with unintended acceleration, but says the safety measure is meant to reassure drivers. Source: [http://www.google.com/hostednews/ap/article/ALeqM5hwIRBT4-YdMT450qxN\\_QccXa\\_o9wD9ESVA300](http://www.google.com/hostednews/ap/article/ALeqM5hwIRBT4-YdMT450qxN_QccXa_o9wD9ESVA300)

**12,000 extension cords, power strips recalled.** The U.S. Consumer Product Safety Commission says a manufacturing company is voluntarily recalling 12,000 extension cords and power strips because they may be fire hazards. The recall of the products from Howard Berger Co. Inc. of Cranbury, New Jersey, involves heavy duty outdoor extension cords and indoor household extension cords and power strips, all of which could have inadequate coating material and too-small copper conductors. All three bear the Brightway brand and were sold at hardware and discount stores around the country between August and October 2009. Recalled outdoor extension cords bear model numbers R2600 through R2615 while the indoor cords have model numbers EE6 through EE20. Powers strips have the MP6DG model number. No injuries have been reported, according to the statement. Anyone who bought the

# UNCLASSIFIED

## UNCLASSIFIED

recalled products should return them to the store where they were purchased for a refund. Source: [http://www.forbes.com/feeds/ap/2010/03/31/business-us-power-strip-recall\\_7478958.html](http://www.forbes.com/feeds/ap/2010/03/31/business-us-power-strip-recall_7478958.html)

**NASA scientists to test Toyota electronics.** A safety board formed by NASA after the 2003 Columbia space shuttle explosion has joined the federal government's inquiry into the causes of sudden acceleration in some Toyota vehicles. The U.S. Transportation Secretary said that engineers from NASA's Engineering and Safety Center (NESC) will help the National Highway Traffic Safety Administration explore potential problems with the electronic throttles in Toyotas. "NASA is an organization that has a great deal of expertise in electronics," the secretary told ABC News, "and they're going to look at the electromagnetic problems that people believe have occurred." "We want Toyotas and all cars to be the safest they can possibly be," he said. "And if these folks can help us get there, then it will be well worth the time and energy and money it takes to get there." Source: <http://abcnews.go.com/Blotter/nasa-scientists-test-toyota-electronics/story?id=10241757>

## **EMERGENCY SERVICES**

**(California) Coast Guard distress call an apparent hoax.** The U.S. Coast Guard searched San Diego Bay and the coastline late Saturday afternoon after receiving an odd radio distress call that apparently turned out to be a hoax. Someone who sounded like a young child said "911 La Mancha" over the radio at 4:57 p.m., said a Coast Guard search and rescue Controller. That phrase is not a standard distress call, he said, but officials launched a search, which is standard in cases when it's not clear whether or not a call is legitimate. A boat and a helicopter searched the bay, Point Loma and the coast up to Encinitas, and found nothing. The search area was based on which radio towers picked up the signal. Source: <http://www.signonsandiego.com/news/2010/apr/03/coast-guard-distress-call-appears-to-be-a-hoax/>

**Audit: Costly FBI computer upgrade drags further.** A Justice Department audit has found the FBI's long-delayed computer upgrade is getting slower and costing more. The FBI's Sentinel program was launched to build a paperless case management system, costing \$425 million. It was supposed to be completed by last December. The system has faced numerous delays and extra costs since. An audit released Wednesday by the Justice Department inspector general said the bureau will not even guess at when it will be done or how much it will cost, though they say it will be more than \$451 million. The FBI has struggled for years to modernize its computer systems. The Bureau director recently told Congress he personally works on the Sentinel project every week, but that has not gotten it back on schedule. The FBI said in a statement that the issues with Sentinel have not hampered investigations, and said the bureau is in talks with the contractor about how to fix the problems. Source: <http://www.google.com/hostednews/ap/article/ALeqM5i2JvGIhU3PYL6w7ETI-Oz7K1TNbAD9EPNCU00>

**Organizations rarely report breaches to law enforcement.** Most organizations hit by breaches that do not require public disclosure do not call in law enforcement — they consider it an exposure risk, with little chance of their gaining any intelligence from investigators about the attack, anyway. The FBI director has acknowledged this dilemma facing organizations that get hacked, noting in a speech at the RSA Conference last month that disclosing breaches to the FBI is the exception and not the rule today. But the FBI will protect victim organization's privacy, data, and will share what information it can from its investigation, he said, rather than continue with the mostly one-way sharing that

## UNCLASSIFIED

# UNCLASSIFIED

organizations traditionally have experienced when dealing with the FBI. The president of the Bay Area CSO Council and CISO at Adobe says different companies have their own rules about reporting to law enforcement. He says the feds have their own communications “protocol” for sharing classified information, but they do not have a standard and confidential way to work with the private sector on breach investigations. And until the feds can work with NDAs, there will not be much back-and-forth between companies and these agencies about breaches, he predicts. Source:

[http://www.darkreading.com/database\\_security/security/attacks/showArticle.jhtml?articleID=224200824&cid=RSSfeed](http://www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=224200824&cid=RSSfeed) DR News

## **ENERGY**

**(Rhode Island) Rhode Island swamped in floods “unprecedented” in state’s history.** Electric utility National Grid pleaded with customers to conserve energy after seven of its substations around the state shut down. CVS pharmacy, headquartered in Woonsocket, announced that flooding had knocked out power to a national computer system affecting prescription services in all 7,000 of its drugstores. The biggest problem in Woonsocket, the mayor said, was a power failure on Main Street that knocked out City Hall phones for a time and traffic lights were out of service. The police were putting up temporary stop signs to control traffic. During an evening news conference, National Grid cautioned customers that 20 additional substations were in danger. If customers do not conserve energy, the company said, it would impose rolling blackouts. Source:

[http://www.projo.com/news/content/flood\\_31\\_03-31-10\\_CEHV0GN\\_v35.405673d.html](http://www.projo.com/news/content/flood_31_03-31-10_CEHV0GN_v35.405673d.html)

## **FOOD AND AGRICULTURE**

**(Texas) Federal government seeks permanent injunction against Texas egg roll manufacturer.** The U. S. Department of Justice, in an action initiated by the U.S. Food and Drug Administration, is seeking a permanent injunction against Chung’s Products LP (“Chung’s”), an egg roll manufacturer in Houston, the company’s president, and the firm’s director of quality assurance. The complaint, filed in the U.S. District Court for the Southern District of Texas, charges the defendants with violating the Federal Food, Drug, and Cosmetic Act (the “Act”) by preparing, packing and holding shrimp egg rolls under insanitary conditions, whereby they may have become contaminated with filth and rendered injurious to health. The complaint concerns Chung’s fish and fishery products. It does not include Chung’s other food products. “The agency has previously warned the company that corrective actions need to be taken in this facility,” the FDA’s acting associate commissioner for regulatory affairs said. The shrimp egg rolls produced by Chung’s are sold in grocery stores and large retail stores nationwide. Source:

<http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm207068.htm>

**Barbecue potato chips recalled due to possible Salmonella contamination.** Lance, Inc. with headquarters in Charlotte, North Carolina is recalling 28,087 cases of Tom’s Barbecue Potato Chips packaged in 1 oz (UPC 021900060406), 2.25 oz (UPC 021900011477) and 8.5 oz (UPC 021900062417) sizes because it has the potential to be contaminated with Salmonella. The product was distributed in 34 states. The product is sold in retail stores and was distributed by direct store delivery by Lance route trucks and by Lance distributors. The product comes in 1 oz, 2.25 oz and 8.5 oz flexible packages. Code dates on the recalled product carry the following expiration dates: May 14 2010, May 21 2010, May 28 2010, Jun 4 2010, Jun 11, 2010, Jun 18 2010, Jun 25 2010, Jul 2 2010, Jul 9 2010, and

UNCLASSIFIED

# UNCLASSIFIED

Jul 16 2010. Source: <http://www.lawyersandsettlements.com/articles/13885/potato-chip-recall-all-tom-bbq.html>

## **GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)**

(Virginia) **Pentagon to increase security measures.** Pentagon officials announced new security measures on Thursday that include more random screening of visitors and Defense Department workers, a wider security perimeter and more lighting around the building's main entrance, after a shooting incident there last month that left the gunman dead and two police officers injured. The changes will be most noticeable at the busy southeast side of the building near the Metro station, according to the Pentagon Force Protection Agency, which has installed more lighting and positioned police officers closer to the station's escalators. "We've had a lot of things in place here since 9/11, but the March 4th incident and other incidents have caused us to really look at this," the PFFA Director said in reference to the March shooting and last year's massacre at Fort Hood, Texas, in which 13 people were fatally shot. Source: <http://www.washingtonpost.com/wp-dyn/content/article/2010/04/01/AR2010040103582.html>

**FBI warns extremist letters may encourage violence.** A federal intelligence note is warning police that an anti-government group's call to remove dozens of sitting governors may encourage others to act out violently. A group that calls itself the Guardians of the free Republics has a plan to "restore America" by peacefully dismantling parts of the government, according to its Web site. As of Wednesday, more than 30 governors had received letters demanding they leave office within three days or they will be removed, according to an internal intelligence note by the FBI and the Department of Homeland Security, which was obtained by The Associated Press. Investigators do not see threats of violence in the group's message, but fear the broad call for removing top state officials could inspire others to act out violently. Source: <http://www.google.com/hostednews/ap/article/ALeqM5hKXtwirU7eHhjk011iMFo7BXjBYQD9EQ7EO1>

(Alabama) **Bomb scare occurs at federal building.** The Federal Building was evacuated for a short time Friday morning while the Gadsden Police Department's bomb squad surveyed a pump sprayer next to the building. The Gadsden fire and police departments responded just before 9 a.m. after someone from the Federal Building, following guidelines established by Homeland Security, notified them of a pump sprayer near the curb on Sixth Street. Sixth Street was closed between Chestnut and Broad streets, although the Federal Building initially remained occupied. After it was determined the bomb squad would survey the sprayer, the building was evacuated. A Gadsden police sergeant examined the sprayer and used tests to determine it contained no explosives. "There wasn't anything there to alert us that it was anything other than what it appeared to be," he said. A bomb made with certain chemicals could be disguised in a sprayer. "We commend them for making the call to take all precautions," the police spokesman said. "Obviously in the times we live in, we have to respond with all caution to any suspicious items or things. We'd rather err on the side of caution." The street was reopened about 11 a.m. Source: <http://www.gadsdentimes.com/article/20100402/NEWS/100409958/1017/NEWS>

UNCLASSIFIED

## UNCLASSIFIED

**US consulate attacked in northwest Pakistan.** Islamist militants unleashed a car bomb and grenade attack against a U.S. consulate in northwestern Pakistan on Monday, killing four people. The multi-pronged strike against the consulate in Peshawar city was the first direct assault on a U.S. mission in the country since 2006. Officials said the four attackers in two vehicles hoped to breach the heavily fortified compound and kill people inside, but they failed to do that and caused only minor damage. They detonated their first suicide vehicle at a checkpoint some 20 meters from the entrance to the consulate, said the Peshawar police chief. The second vehicle, which was carrying a larger amount of explosives, was stopped at another security barrier some 15 meters from the entrance. "The driver had no option, but to detonate the vehicle right there," he said. The second blast killed two militants wearing suicide vests who were walking ahead of the pickup truck. Some officials and witnesses reported a third or possible fourth explosion. The attackers who fired at the consulate were wearing security uniforms. The four people killed in the attack included three security personnel and one civilian, said the police chief. Two of the security personnel were employed by the consulate, said the embassy. The third was a Pakistani paramilitary soldier, said a police official. The Pakistani interior minister said the Pakistani Taliban claimed responsibility for the attack. Source:

<http://www.google.com/hostednews/ap/article/ALeqM5hkiMxbHNNH0BqgpWA2ZG6VD6wVTmAD9ET1GU00>

**GAO concerned over UAS infrastructure.** Satellite control of unmanned aircraft systems is potentially open to disruption thanks to lack of a backup relay site, according to the Government Accountability Office. The number of unmanned aircraft in use by the Defense Department had skyrocketed over the past decade, from fewer than 50 in 2000 to more than 6,800 in October 2009. However, the inventory might be outpacing DoD's ability to comprehensively support it with a robust communications infrastructure, as well as personnel training and facilities, the GAO finds. Air Force officials told GAO auditors they're taking steps to establish a redundant satellite relay site to support UAS missions in the event of disruptions at the current location. The GAO is concerned, however, that the effort is not scheduled for completion until 2012 and that the Air Force lacks a formal backup plan for continuity of operations should the current satellite relay site be disrupted. Source:

<http://www.fiercegovernmentit.com/story/gao-concerned-over-uas-infrastructure/2010-04-01>

**The military services are working out security policies for thumb drive use.** The Air Force does not expect to have a policy governing the use of flash media such as thumb drives in place until October and will allow their use only under carefully controlled circumstances, the service's team leader responsible for flash media said. The Army and Navy could not provide a date when their flash media policies would go into effect, but spokesmen for both services emphasized they are taking a slow and deliberate approach, evaluating technical as well as financial issues. The Strategic Command, which has responsibility for cybersecurity throughout the Defense Department banned the use of flash media on military computers and networks in November 2008 because adversaries had found ways to use gadgets such as thumb drives to infect Defense networks with software containing malicious bugs. In February, STRATCOM revised its policy to allow flash media as a "last resort for operational requirements." The revised policy required the services to develop their own guidelines. Source:

[http://www.nextgov.com/nextgov/ng\\_20100401\\_1208.php](http://www.nextgov.com/nextgov/ng_20100401_1208.php)

**(Nevada)Capitol adds security after threats.** State workers and visitors to the Nevada Capitol arrived Wednesday morning to find all but the front door locked and metal detectors for both packages and

## UNCLASSIFIED

## UNCLASSIFIED

people set up at the entrance. The Capitol was locked down late Tuesday after the FBI advised the governors of all 50 states they would be receiving letters from an extremist group demanding their resignations, according to the deputy chief of staff to the Nevada governor. The chief of staff said the decision was to “err on the side of caution” and implement tough security measures. The Capitol houses offices of the governor, lieutenant governor, secretary of state, controller and treasurer. The letters reportedly advise governors that, if they do not resign, members of the group will “commandeer” their offices. It was received by the Capitol Police at noon Monday and immediately turned over to FBI investigators. The letters are apparently from an organization allied with Sovereign Citizens, which the Anti-Defamation League identifies as a collection of anti-government groups advocating an anarchist ideology. Its followers believe every level of government in the United States is illegitimate and should be eliminated. Source:

<http://www.nevadaappeal.com/article/20100401/NEWS/100339874/1001&parentprofile=1058>

**U.S. Navy captures pirates after exchanging fire.** Somali pirates fired at a U.S. Navy warship on Thursday, in one of the more brazen attacks of armed men in skiffs who prey upon vessels plying the sea lanes of the Indian Ocean. The USS Nicholas took fire just after midnight from a small skiff, according to a statement from U.S. Africa Command. The 450-foot frigate, which was patrolling west of the island nation of the Seychelles, fired back, chased down the skiff, and detained three people on board, according to a spokesman for U.S. Naval Forces Africa. The warship had received a tip from other U.S. ships that suspected pirates might be in the area, he said. After the exchange of fire, officials confiscated ammunition and sunk the boat. The naval destroyer then overtook a second ship that naval officials believe is a so-called pirate mother ship, and arrested two suspects on board. A third ship escaped. Reached by phone in the central Somali pirate town of Xaradheere, a fellow Somali pirate said that he had spoken with his colleagues by satellite phone to glean more information. He did not know why they had attacked the warship. But in the dark, the pirates may have mistaken the warship for the many cargo ships that have brought them lucrative ransoms. The Nicholas is attached to the U.S. Naval Forces Africa, the naval component of US Africa Command, or Africom, and has been patrolling the waters off of East Africa since late December. Source:

[http://online.wsj.com/article/SB10001424052702304539404575157663093991350.html?mod=WSJ\\_hpp\\_MIDDLENexttoWhatsNewsThird](http://online.wsj.com/article/SB10001424052702304539404575157663093991350.html?mod=WSJ_hpp_MIDDLENexttoWhatsNewsThird)

**(Florida) Eglin Air Force Base examining suspected bomb.** A suspected bomb left outside a Santa Rosa County Sheriff’s Office precinct was being examined Tuesday by explosive-ordnance-disposal personnel at Eglin Air Force Base. A Sheriff’s Office spokesman said Tuesday that the suspected bomb had been turned over to explosives experts at Eglin, and the Sheriff’s Office had not been informed whether the device was dangerous. A man brought the unidentified device to the Sheriff’s Office building on the 1300 block of College Parkway after finding it in the Beaver Pond area Monday afternoon. Deputies blocked College Parkway and evacuated the precinct building as a precaution while waiting for a bomb-disposal team from Eglin. Source:

<http://www.pnj.com/article/20100331/NEWS01/3310333/1006/NEWS01/Eglin-Air-Force-Base-examining-suspected-bomb>

**(Connecticut) Bomb scare clears out courthouses.** Traffic came to halt downtown for about an hour and a half Tuesday after police evacuated three New Haven courthouses because of a bomb threat. The threat came shortly before 4 p.m. Police with bomb-sniffing dogs entered the courthouses starting around 5 p.m. Yale, New Haven, and state police, as well as judicial and federal marshals,

## UNCLASSIFIED



## UNCLASSIFIED

were also present at the scene. State police said they did not find any suspicious items in the courthouses. "We responded in an appropriate manner," the City Hall spokeswoman said Tuesday afternoon. "An evacuation took place, and an investigation is ongoing." Source:

<http://www.yaledailynews.com/news/city-news/2010/03/30/bomb-scare-evacuates-courthouses/>

**(Texas) Colleges evacuated for bomb threat.** Texarkana College and Texas A&M University-Texarkana buildings were evacuated Tuesday after a bomb threat but no potential explosive had been found as of presstime. The call was received about 8:15 p.m. at the 911 dispatch center in the Bi-State Justice Center, said the TC president. Bi-State officials notified TC officials about the threat. City police and fire departments arrived on scene to assist. Source:

<http://www.texarkanagazette.com/news/localnews/2010/03/31/colleges-evacuated-for-bomb-threat-50.php>

**U.S. embassy in Nigeria raises security alert status.** The United States embassy in Nigeria said Wednesday it had raised its security alert status because of "continuing worldwide terrorist threats against U.S. citizens." An email sent to Americans living in Nigeria did not give details of the threats. "Due to continuing worldwide terrorist threats against U.S. citizens, U.S. government facilities, and U.S. interests, the U.S. Mission in Nigeria, which includes the U.S. Embassy in Abuja and the U.S. Consulate General in Lagos, has increased its alert status," the notice said. Source:

<http://www.reuters.com/article/idUSTRE62U1CV20100331>

## **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**First iPad jailbreak demoed.** A iPhone Dev Team member has released a video showing a rough demo of a jailbreak that's given him access to the iPad's software inner workings. While it's more of a developmental hack than a full-functioning, consumer-grade jailbreak at this point, it's only matter of time before iPad amateurs will be able to unleash the tweak on their own devices. And, of course, that means third-party application installers like Cydia are but a touch or two away. How does the jailbreak work? The details are unclear. However, since the jailbreak is allegedly based off of a jailbreak for the iPhone called, "Spirit," written by a developer called Comex, it's safe to say that the methods used will be similar when the consumer-grade jailbreak is unleashed. Source:

<http://www.pcmag.com/article2/0,2817,2362241,00.asp>

**Botnets drive the rise of ransomware.** Ransomware is the dominating threat with nine of the detections in the malware top ten list resulting in either scareware or ransomware infesting the victim's PC. Fortinet observed the primary drivers behind these threats to be two of the most notorious botnet "loaders" - Bredolab and Pushdo. Another important finding is the aggressive entrance of a new zero-day threat in FortiGuard's top ten attack list, MS.IE.Userdata.Behavior.Code.Execution, which accounted for 25 percent of the detected activity last month. Key threat activities for the month of March include: SMS-based ransomware high activity, botnets, and zero day attacks. A new ransomware threat, DigiPog, is an SMS blocker using Russian language, locking out a system and aggressively killing off popular applications like Internet Explorer and Firefox until an appropriate code is entered into a field provided to the user. Sasfis, another botnet loader, moved up eight positions in our Top 100 attack list from last month, landing just behind Gumblar and Conficker network activity in the fifth position. Sasfis is just the latest

## UNCLASSIFIED

## UNCLASSIFIED

example of simplified botnets, which are used heavily for malicious business services (crime as a service). A new zero-day threat aggressively entered FortiGuard's top ten attack list: MS.IE.Userdata.Behavior.Code.Execution - this exploit triggers a vulnerability in Internet Explorer, making remote code execution through a drive-by download (no user interaction required) possible. Source: <http://www.net-security.org/secworld.php?id=9095>

**Gaming apps increase spam, phishing by 50 percent.** Gamers beware – the next person you add to your gaming social network could be a spammer or phisher. A new report from BitDefender found that gaming applications increase spam and phishing by more than 50 percent in social networks. While most users of social networks are somewhat selective in who they add to circle of friends – filtering out those they suspect to be spammers – gamers often willingly add suspicious friends in an effort to expand their player community. Some entertainment apps require users to amass a large number of friends and supporters in order to attain high scores, prompting players to add people they might not normally add. The most “successful” spammers are those that copy existing profiles. Source: <http://www.pcmag.com/article2/0,2817,2362134,00.asp>

**Weak passwords stored in browsers make hackers happy.** Nearly a quarter of people (23 percent) polled in a survey by Symantec use their browser to keep tabs on their passwords. A survey of 400 surfers by Symantec also found that 60 percent fail to change their passwords regularly. Further violating the ‘passwords should be treated like toothbrushes’ maxim (changed frequently and not shared), the pollsters also found that a quarter of people have given their passwords to their spouse, while one in 10 people have given their password to a ‘friend’. Password choices were also lamentably bad. Twelve of the respondents admitted they used the phrase ‘password’ as their password while one in ten used a pet’s name. The name of a pet might easily be obtained by browsing on an intended target’s social networking profile. Eight percent of the 400 respondents said they used the same password on all their online sites, a shortcoming that means a compromise of one low-sensitivity account hands over access to a victim’s more sensitive webmail and online banking accounts. Source: [http://www.theregister.co.uk/2010/03/30/password\\_security\\_still\\_pants/](http://www.theregister.co.uk/2010/03/30/password_security_still_pants/)

**Hacker finds a way to exploit PDF files, without a vulnerability.** A security researcher has managed to create a proof-of-concept PDF file that executes an embedded executable without exploiting any security vulnerabilities. The PDF hack, when combined with clever social engineering techniques, could potentially allow code execution attacks if a user simply opens a rigged PDF file. A researcher who found the flaw explained: “I use a launch action triggered by the opening of my PoC PDF. With Adobe Reader, the user gets a warning asking for approval to launch the action, but I can (partially) control the message displayed by the dialog. Foxit Reader displays no warning at all, the action gets executed without user interaction.” Although PDF viewers like Adobe Reader and Foxit Reader does not allow embedded executable (like binaries and scripts) to be extracted and executed, the researcher discovered another way to launch a command (/Launch /Action), and ultimately run an executable he embedded using a special technique. The researcher said Adobe’s PDF Reader will block the file from automatically opening but he warned that an attacker could use social engineering tricks to get users to allow the file to be opened. Source: <http://blogs.zdnet.com/security/?p=5929>

**Security researchers scrutinize search engine poisonings.** The techniques used by scammers who automate search engine manipulation attacks themed around breaking news to sling scareware have been unpicked by new research from Sophos. A research paper published on March 31 by Sophos

## UNCLASSIFIED

## UNCLASSIFIED

researchers lifts the lid on the search engine optimization techniques used by hackers to hook surfers into their scams. Attackers use automated kits to apply blackhat SEO methods – cynically exploiting tragic or salacious breaking news stories – to subvert searches in order to point surfers towards scareware download portals or other scams. The deaths of celebrities, the release of Google Wave, and the marital strife of a popular celebrity are among the topics which have been used as themes for these attacks in the past. Just about any high-profile breaking news story is fodder for the crooks, so it came as little surprise that the deaths of 39 people in the Moscow metro suicide bombings on March 29 have also become themes for the latest run of black-hat SEO techniques. Cybercrooks behind the scams do not simply sit watching Google Trends or trending topics on Twitter, however. The process is increasingly becoming automated. Source:

[http://www.theregister.co.uk/2010/03/31/search\\_poisoning\\_dissected/](http://www.theregister.co.uk/2010/03/31/search_poisoning_dissected/)

### **NATIONAL MONUMENTS AND ICONS**

**(Maryland) Fire damages historic hotel.** A landmark hotel in Emmitsburg, Maryland, that was one of the last structures that burned in the “Great (Emmitsburg) Fire of 1863” has burned again, and one person has been arrested. More than 100 to 125 firefighters descended on an early Saturday morning fire that severely damaged more than half of the four-story, East Main Street Emmitsburg Hotel, a structure whose history can be traced back to before the mid-1800s. The Emmitsburg Hotel, actually a 17-unit apartment building, caught fire around 6 a.m. Saturday, resulting in fire companies within a half hour distance either sending in manpower and equipment to the scene or covering for firefighting companies that responded. The burning structure was surrounded by firefighters from Emmitsburg, Gettysburg, Walkersville, and Taneytown before it was brought under control three hours later around 9 a.m. There were no serious injuries reported. The fire left 28 occupants homeless. A 43-year-old man, a resident of the Hotel, has been charged with arson and malicious burning, according to the state Fire Marshal’s Office. Investigators say the man was trying to commit suicide. The property is also known for its historical visitors such as Francis Scott Key — the composer of the National Anthem — once delivered a speech from the hotel’s balcony, as did President William Henry Harrison. The old hotel sustained more \$1 million in damages in Saturday’s fire according to the latest estimate. Source:

<http://www.gettysburgtimes.com/articles/2010/04/05/news/local/doc4bb9c0a985265527960224.txt>

**(Oregon) Web site included threats to trail hike near river.** An Ashland environmental group was put on alert after a man posted threatening messages on a gold mining Web site suggesting that its members be shot with a high-powered rifle during a hike along the Rogue River. KS Wild workers discovered the post at oregongoldhunters.com on March 14, a week after they hosted a public hike through federal land along the Lower Rogue River trail. “It was pretty disturbing to read such a threat after the hike,” said KS Wild’s conservation director. “Thankfully there was no violence, but we are taking these threats seriously.” The man who posted the message is listed as a moderator on the Oregon Gold Hunters Web site. The message suggested those who follow discussion threads on the site should show up during the KS Wild hike and confront the group. Another person replied that this would be a “good idea.” The messages prompted KS Wild to contact the Federal Bureau of Investigation and the Oregon Attorney General. An Oregon U.S. Senator denounced the messages and called on law enforcement agencies in Jackson and Josephine counties to investigate the matter. Local environmental groups have been at loggerheads with miners for several years over the issue of

## UNCLASSIFIED

# UNCLASSIFIED

whether public rivers and streams are open for gold dredging by private entities. Source: <http://www.mailtribune.com/apps/pbcs.dll/article?AID=/20100331/NEWS/3310320>

## **POSTAL AND SHIPPING**

**(Texas) 2 suspicious devices found in east Texas mailboxes.** Two more possible pipe bombs were found in east Texas mailboxes Tuesday, even as the U.S. Bureau of Alcohol Tobacco, Firearms and Explosives (ATF) said it would add resources to investigate a series of explosive devices found in that part of the state in recent weeks. A U.S. Postal Inspector said the latest devices were found in a mail collection box in Longview and in a residential mailbox in a subdivision on Lake Cherokee, about 15 miles southeast of Longview. An apparent pipe bomb was found in the mail collection box at an office building just north of downtown Longview about 4:40 p.m. Tuesday, she said. The office building was evacuated. Longview is about 120 miles east of Dallas. The Lake Cherokee device, also apparently a pipe bomb, was found about 12:40 p.m. Tuesday. Both devices were rendered safe and sent to a laboratory operated by the ATF for testing. The public was not threatened, she said. ATF and the U.S. Postal Inspection Service have raised to \$25,000 the reward they are offering for information leading to the arrest and conviction of those who have planted the mailbox devices. Source: <http://www.dallasnews.com/sharedcontent/APStories/stories/D9EPALA02.html>

## **PUBLIC HEALTH**

**Health Information Security Conference to run May 11-12 in D.C.** The National Institute of Standards and Technology (NIST) is co-hosting a conference to explore the current health information technology security landscape and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The conference on "Safeguarding Health Information: Building Assurance through HIPAA Security," presented in collaboration with the Department of Health and Human Services (HHS) Office for Civil Rights, will be held on May 11 and 12, 2010, in Washington, D.C. This conference will provide a forum to discuss the present state of health information security, and practical strategies, tips and techniques for implementing the security requirements of HIPAA. Industry panels will discuss breach notification rules and the state of compliance with the Security Rule. The meeting is expecting to draw hundreds of HIPAA security rule implementers; security, privacy and compliance officers; assessment teams and audit staff. Source: <http://www.newswise.com/articles/health-information-security-conference-to-run-may-11-12-in-d-c>

**Hackers could target medical devices.** Although no such attacks have yet been reported, medical devices could be susceptible to hackers, and a thorough security analysis should be done as part of FDA approval, researchers argue. Premarket regulatory evaluation should include a risk-based security assessment depending on the nature of the device and the perceived threat of a security compromise, said a member of Beth Israel Deaconess Medical Center, in Boston, and a member of the University of Washington in Seattle. They made their argument in a "Perspective" article in the April 1 issue of the New England Journal of Medicine. "We think medical device security should be improved before there is a widespread incident, rather than waiting for the incident to occur and then acting," one member said in an e-mail to MedPage Today. "It is very difficult to add on security after the fact." The authors said that in terms of security risks, medical devices are like "the drug supply of a generation ago." The contributors said computer security specialists "see weaknesses in

# UNCLASSIFIED

## UNCLASSIFIED

the current technology of many medical devices.” Potential vulnerabilities include unauthorized device reprogramming and data extraction. Or hackers could flood a device with information so that normal communication fails to reach it. There are also tactics to prematurely drain a device’s battery and eventually reduce its lifespan by repeatedly awakening it from a sleep state. Source:

<http://www.medpagetoday.com/ProductAlert/DevicesandVaccines/19350>

**(Texas) Theft of pharmaceutical cargo bound for H-E-B warehouse in San Marcos is part of national trend.** A truckload of over-the-counter pharmaceuticals that was bound for an H-E-B grocery warehouse in San Marcos was stolen in early March in the Dallas area. The theft of the cargo, valued at \$400,000, is part of a larger trend of high-stakes heists across the country involving millions of dollars worth of pharmaceutical shipments, experts say. The theft of prescription drugs, from blood thinners to insulin, “has exploded in the last five years,” a professor at the University of Texas College of Pharmacy and an expert in prescription drug theft and diversion, recently told The Hartford Courant. In the case of the pharmaceuticals headed for San Marcos, an entire truckload belonging to Perrigo Co. was swiped. The shipment was en route from a Perrigo distribution center in Martin, Michigan, to the HEB warehouse. Perrigo is one of the biggest U.S. makers of generic and private-label over-the-counter pharmaceuticals and supplements. The Perrigo load contained the hair re-growth treatment minoxidil, quit-smoking nicotine gum and lozenges, and various over-the-counter vitamins and nutritional supplements, according to an alert from the Pharmaceutical Cargo Security Coalition. The heist happened in the first couple of days of March. The alert was reported by the Secure Pharma Chain Blog and SecuringPharma.com. “Police have evidence that the driver was involved and have enough information to file theft cases on him and a second individual,” the chairman of the SouthWest Transportation Security Council, told Examiner.com. States that are considered hot spots for pharmaceutical cargo theft are Tennessee, Pennsylvania, Florida, and California. Source: <http://www.examiner.com/x-37614-Austin-Market-Examiner~y2010m3d31-Theft-of-pharmaceutical-cargo-bound-for-HEB-warehouse-in-San-Marcos-is-part-of-national-trend>

## **TRANSPORTATION**

**(Oklahoma) Man threatens to detonate bomb at Tulsa International Airport.** Officers at the Tulsa International Airport chased down and arrested a man who threatened to detonate a bomb at a security checkpoint Sunday night. The man, 42, is accused of making the bomb threat to a Transportation Security Administration employee about 8:20 p.m. Authorities allege that the man walked to the checkpoint and told the worker that he had a bomb and detonator in a gym bag that he was carrying. He then threatened to start an explosion before running away from the checkpoint, according to his arrest report. Source: [http://www.newsok.com/man-threatens-to-detonate-bomb-at-tulsa-international-airport/article/3451534?custom\\_click=pod\\_headline\\_crime](http://www.newsok.com/man-threatens-to-detonate-bomb-at-tulsa-international-airport/article/3451534?custom_click=pod_headline_crime)

**TSA steps up security on flights.** The TSA is implementing enhanced security measures on international flights to the U.S. that override those put into place after the December 25 attempted bombing of a Northwest Airlines flight. “Multiple random layers of security, seen and unseen” will apply to all passengers on international flights to the U.S. worldwide, according to the U.S. Homeland Security Department Secretary, who announced the new protocols Friday. Enhanced measures could include explosives trace detection, use of advanced imaging technology, canine teams and pat-downs. The new, more flexible protocols are based on real-time, threat-based intelligence and the

## UNCLASSIFIED



## UNCLASSIFIED

most current information available to the U.S. The stepped-up measures are part of a larger effort: the Secretary has been working with the International Civil Aviation Organization on an initiative aimed at strengthening the global aviation security system against terrorism. To that end, she has been participating in security summits worldwide, including those in Tokyo and Spain, forging collaborative agreements with numerous nations aimed at adopting more effective ways of identifying and thwarting terrorist threats. Goals include raising security standards, enhancing intelligence-gathering and sharing, as well as developing and implementing, security technologies.

Source:

[http://www.aviationweek.com/aw/generic/story\\_channel.jsp?channel=comm&id=news/avd/2010/04/05/08.xml](http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=comm&id=news/avd/2010/04/05/08.xml)

**(Vermont) Fighter jets called to VT after distress signal.** Officials say an inadvertently activated distress call from a private plane scrambled two fighter jets to Middlebury, Vermont. The North American Aerospace Defense Command says two F-15 fighter planes were sent to Middlebury on Friday after officials received a distress signal indicating the plane could have been hijacked or there was an in-flight emergency. NORAD officials say the plane landed at the Middlebury State Airport on Friday afternoon without incident before the jets could reach the area from the Massachusetts Air National Guard Base in Westfield. Source:

<http://wbztv.com/wireapnewsma/Fighter.jets.called.2.1611662.html>

**(New York) Insecurity cams? About half in NYC don't work.** About half the 4,313 security cameras installed along New York City's subways are not seeing a thing — a blind spot in the crime and terrorism safety net for the nation's largest city. "A lot of those cameras do not work, and maybe someday we're going to get very badly hurt because of it," the New York Mayor said Tuesday. While cameras are out of commission in the subway, the cash-strapped Metropolitan Transportation Authority has also been forced to cut police patrol shifts on major bridges and tunnels on the weekends. The problem of missing video came to light after two men were stabbed to death on the subway — and there was no camera installed in the station to catch an image of the killer. The New York Police Department says it does not depend on the surveillance cameras set up by the MTA — instead, officers patrol the subways and set up random bag searches in stations around the city. The NYPD is installing thousands of cameras around the city and is using private surveillance installed in major buildings as part of a massive security initiative. In addition, 500 specialized cameras are in place — an image from one of those cameras led officers to a suspect wanted in the brutal assault of a woman in a bar a few weeks ago. Meanwhile, about 600 agents stationed in the subways have been laid off as a result of the budget. A working, comprehensive surveillance system for the city's many bridges and automobile tunnels is monitored 24 hours a day. But some of the weekend patrol shifts for officers who regularly patrol the bridges — and who could respond to a threat within minutes — have been eliminated at the Queens Midtown Tunnel and the Verrazano Narrows Bridge, which connects Brooklyn and Staten Island. The vice president of the Bridge & Tunnel Officers Benevolent Association said the cuts will make it more difficult to catch any miscreants. "The Verrazano is a 2 1/2-mile long bridge. The monitoring system is on Staten Island. If an alarm goes off, or someone sees something, dispatching someone over to Brooklyn could mean the guy gets away," he said. The MTA said that the plan has been evolving since the Sept. 11 terrorist attack, and that additional funding will be made available to add more cameras in priority areas. Source:

[http://www.google.com/hostednews/ap/article/ALeqM5jZXf1jHyUW-S4Hlf\\_Fdyp72B7KcwD9EP7SOO0](http://www.google.com/hostednews/ap/article/ALeqM5jZXf1jHyUW-S4Hlf_Fdyp72B7KcwD9EP7SOO0)

UNCLASSIFIED



# UNCLASSIFIED

**(Georgia) Bomb scare at airport.** The Southwest Georgia Regional Airport had a bomb scare early Tuesday morning. Airport security found an unattended bag by the flags just outside of the airport entrance. When security could not confirm to whom the bag belonged, they called the fire department and police bomb unit. The airport director says the security guards shut down the airport and evacuated the few employees working while they waited on police to arrive. "The bomb unit decided to blow up the bag to see what was inside of it because they couldn't find out who owned the bag. They found out that it was a suitcase with clothes in it," the director said. The 6:30 a.m. morning flight was delayed by one hour due to the bomb scare, and officials say everything is back to normal at the airport. Source:

<http://www.mysouthwestga.com/news/story.aspx?list=~\news\lists\local&id=437058>

## **WATER AND DAMS**

Nothing Significant to Report

## **NORTH DAKOTA HOMELAND SECURITY CONTACTS**

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **Fusion Center (24/7):** 866-885-8295; email: [ndslic@nd.gov](mailto:ndslic@nd.gov) ; FAX: 701-328-8175

**State Radio:** 800-472-2121 **Bureau of Criminal Investigation:** 701-328-5500 **Highway Patrol:** 701-328-2455

**US Attorney's Office Intel Analyst:** 701-297-7400 **Bismarck FBI:** 701-223-4875 **Fargo FBI:** 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security [kihagel@nd.gov](mailto:kihagel@nd.gov), 701-328-8168



UNCLASSIFIED

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**